Exhibit 45

Excerpts of SW-SEC00166790

solarwinds msp

MSP Products Security Evaluation

confidential

July 2019

Stas Starikevich, Wojciech Pitera

Detailed discussion

Asset management (identify)

Hardware assets (including cloud systems)
The collection of asset/inventory information is inconsistent and varies from Product to Product. This makes it very difficult to manage the company's asset, throughout its life cycle. IT asset management methodology and best practices would need to be implemented to help standardize the process across the board.

In order to have a successful automated security operations (i.e. network scanning), it is recommended we establish a common policy and a central repository, where, at the very least, utilised IPs can be obtained. Ideally the inventory should be maintained in an automated way and have software relationship metadata to allow product/service correlation.

Software assets
The Majority of the products don't have a policy defining what and how software assets should be catalogued. While there is Product & Technology Catalogue within SolarwWinds, it does not seem to be actively maintained and appears to be missing significant amount of assets.

It is crucial for security operations to have consistent manner of maintaining software assets to allow automation. Current process of creating, for example, Checkmarx scans is completely separated from Product Catalogue and seems to be, only, usable for given context.

It is recommended to define appropriate global policy regarding asset inventory and establishing a single space where that would be stored. Ideally asset inventory would include all required software metadata (jira, repository, programming language, department, team, etc.) to allow automated operations and become single source of truth for other processes.

Communication and data flows are mapped

Design documentation overall is lacking and unstructured for the majority products. In addition, there is no governance in place to help provide consistency. These are crucial for threat modelling & other security activities in SSDLC. This should be covered by architecture, as part of the SSDLC process being formed.

Resources are prioritized based on their criticality and business value

No formal policy or process exists to prioritize resources (hardware and software) which is fundamental for proper risk assessment and effective response strategies.

Business environment (identify)

Dependencies and critical functions for delivery of critical services are established

Lack of policies – Very little guidance and documentations, if any. A SPOF analysis exercise was done for each product.

Resilience requirements are established for critical services

No policies, huge room for improvement – Should be mandatory for all critical services, which is majority of them (implementing SLO/SLI)

Risk assessment (identify)

Asset vulnerabilities are identified and documented

Each product seems to have its own ways of marking security issues that do not follow recently established SW standards.

Threat and vulnerability information is received from external sources

Currently, there is no formal process in place for reporting purposes. It is recommended to have a process/framework to help provide guidance, specific to job responsibility/Role … (i. e. DevSecOps, Ops ?) – A Pre-requirement to have a policy to maintain proper 3rd party asset list, OS versions utilised etc, to have data to work with.

Threats internal and external are identified and documented

No threat modelling nor analysis is performed as part of any process (except MSP Backup Engineering). Has multiple pre-requirements to be implemented (external software assets, 3rd party systems list etc)

Potential business impacts and likelihoods are identified

Room for improvement in area of identified vulnerabilities – New SWI global process established but not yet implemented in MSP (RMM piloting). Pre requirement to have threat analysis performed to claim coverage in full scope.

Threats, vulnerabilities, likelihoods and impacts are used to determine risk

No coverage due to missing pre requirements.

Risk responses are identified and prioritized

Partially covered by not fully implemented CVSS scoring providing prioritization of vulnerabilities (only). No official policy nor procedure. To be defined as part of SSDLC and to include threats.

Risk management strategy (identify)

Risk management processes are established

Recommendations:

- Define resilience requirements and service level objectives
- Execute SPOF analysis (define goals, design the plan to achieve those goals)
- Incorporate steps from the plan into the product backlog

Anomalies and events (detect)

Some baseline network operations and expected data flows established allowing some limited tracking of unexpected events, but no official policies/procedures and are not really security focused.
Logs kept from multiple sources, but often difficult to correlate.
Impact analysis rarely executed (if ever).
No policies or processes defined.

Recommendations:

- Create policy and processes for static code analysis tools (onboarding, handling detections)
- Log and ship to papertrail all the shell (command line) activity on the servers
- Mandate the AV on the Windows systems (now it's not enforced)
- Implement system to detect unauthorized processes and files on the production infrastructure

Security continuous monitoring (detect)

Not covered under any policy/procedure.

Detection processes (detect)

Not covered under any policy/procedure.

Response (planning, communication, analysis, mitigation, improvements)

Response partially covered with current IRP process we use from April 2018.

Recover (recovery planning, improvements, communication)

Not covered under any policy/procedure.